User Manual

Device Lock®

Ecora Software Inc.

Contents

Using this manual 3

1. Overview 4

1.1 General Information 4
1.2 Security 5
1.3 Requirements 6
1.4 Main Purpose 7

2. Device Lock Manager 8

2.1 Installation 8
2.2 Interface 9
2.3 Main Dialog 10
2.4 Permissions Dialog 13
2.5 Batch Permissions 16
2.6 Flush Buffers 17

3. Device Lock Service 18

3.1 Installation 18

Appendix 22

Permission Examples 22

Copyright ©1997-2004 SmartLine Inc. All rights reserved.

Using this Manual

This manual assumes you're familiar with basic functions like click, right-click, and double-click, and that you're familiar with the basics of the operating system you're using. This manual also assumes that you have basic network knowledge as well as the ability to install a Local Area Network (LAN). We strongly recommend reading this manual very carefully and thoroughly.

This manual uses the following conventions:

- *Italics* for file names and paths.
- **Bold** for buttons, menus, menu items, and other named user interface items.
- ***Bold Italics*** for notes and comments.
- Keyboard keys with a plus sign separating keys that you press simultaneously. For example: press CTRL+ALT+DEL to restart your computer.

Overview

1.1 — General Information

Preventing the introduction of inappropriate software and data is important when trying to protect and administer a company's computer network. The traditional solution has been a physical lock on the floppy drive. Device Lock eliminates the need for physical locks and has a number of advantages.

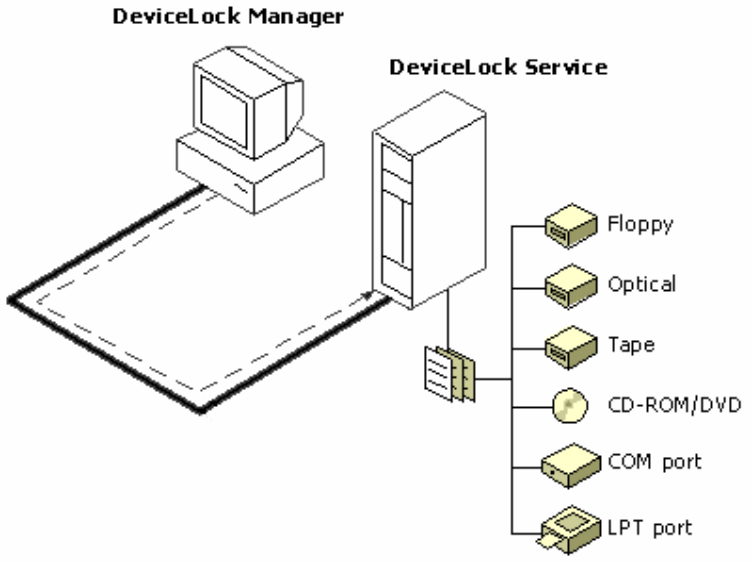
Device Lock is easy to install. Administrators can have instant access from remote computers when necessary. There are no physical keys to store and manage.

The administrator of the machine or domain can designate user access to floppy drives, CD-ROM drives, other removable media, tape drives, WiFi, and Bluetooth adapters, or USB, FireWire, infrared, and serial and parallel ports. Any types of the file systems are supported.

Device Lock consists of two parts: Device Lock Service (*dlservice.exe*) and Device Lock Manager (*dlmanager.exe*).

Device Lock Service is the core of Device Lock. Device Lock Service is installed on each client system, runs automatically, and provides device protection on the client machine while remaining invisible to that computer's local users.

Device Lock Manager is the control interface systems administrators use to remotely manage each system that has Device Lock Service.



Copyright ©1997-2004 SmartLine Inc. All rights reserved.

1.2 — Security

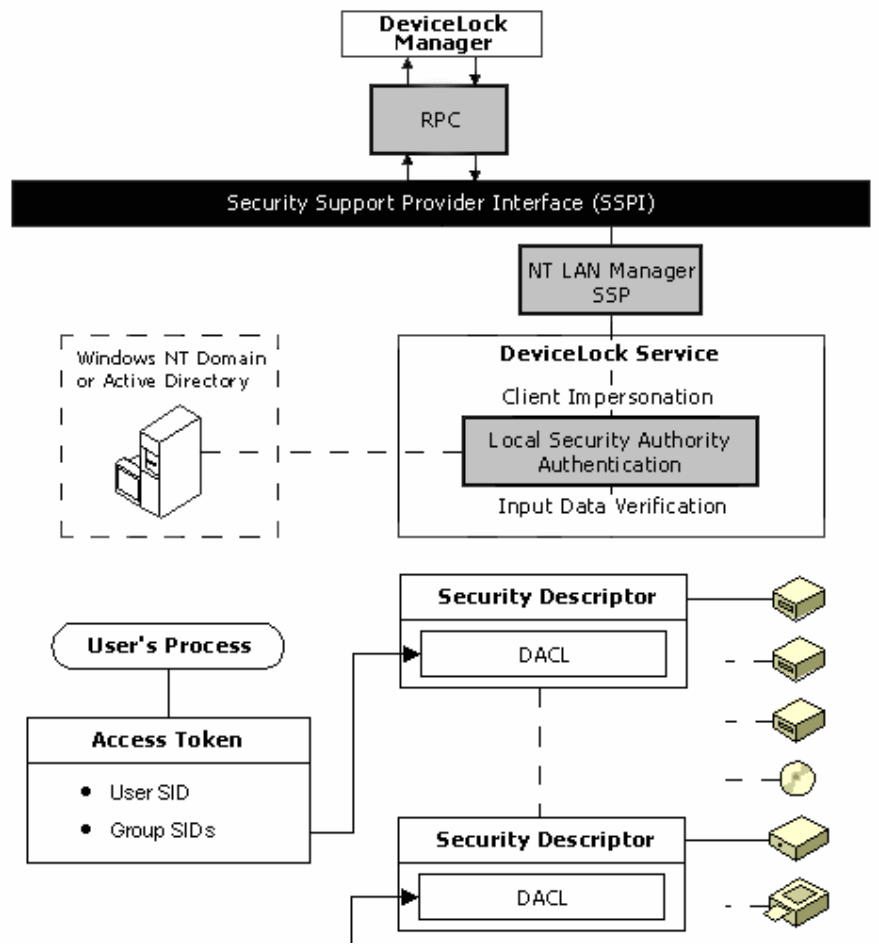
Reliable access control functionality is the primary focus of Device Lock.

Device Lock uses Remote Procedure Call (RPC) technology for communication between the service and the manager. It uses the Windows user-level security subsystem for authentication.

Device Lock's security is integrated into the Windows access control subsystem. Remote computers with an installed Device Lock Service can only be accessed by someone with administrator privileges.

Because Device Lock uses standard protocols, it operates like any other Windows administrative tool, such as User Manager, Server Manager, Event Viewer, etc.

The Device Lock Service on each client machine checks all input data for size and type, eliminating buffer overflow attacks.



Copyright ©1997-2004 SmartLine Inc. All rights reserved.

1.3 — Requirements

Device Lock works on any computer using Windows NT/2000/XP or Windows Server 2003.

To install and use Device Lock, you MUST have administrative privileges.

If you are going to use Device Lock only on a local computer, you must have local administrative privileges.

If you are going to use Device Lock throughout your network, you must have domain administrator privileges.

If you want to use Device Lock on your network, you must have a functioning TCP/IP network protocol. However, Device Lock can also work on stand-alone computers. A network is needed only if you want to control Device Lock Service from a remote computer.

1.4 — Main Purpose

- Device Lock gives network administrators control over which users can access what devices (floppies, Magneto-Optical disks, CD-ROMs, DVDs, ZIPs, USB, FireWire, infrared, serial and parallel ports, tape devices, WiFi, and Bluetooth adapters, etc.) on a local computer.

- Once Device Lock is installed, administrators can control access to floppies, CD-ROMs, or other devices, including access control by the time of day and day of the week.

- Device Lock enhances access control for Windows system administrators and helps control removable disk usage.

- Device Lock can protect network and local computers against viruses, Trojan horses, and other malicious programs often introduced by removable media.

- Device Lock can protect disks from accidental or intentional formatting.

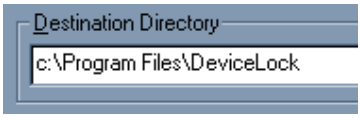
- Device Lock allows administrators control over which users can eject what removable devices.

- Network administrators can also use Device Lock to flush a storage device's buffers.

2.1 — Installation

Device Lock Manager can be installed to any computer running Windows NT/2000/XP or Windows Server 2003.

To install Device Lock Manager, run Setup (*setup.exe*).



Device Lock Manager installs to the directory of your choice. Setup tries to find a Device Lock Manager installation and, if one exists, Setup suggests you install Device Lock Manager to the same directory. If a previous installation does not exist, Setup suggests you install Device Lock Manager to the Program Files directory on the system drive (e.g. *C:\Program Files\ Device Lock*). You can select another directory for installation.

You have two choices: install both Device Lock Manager and Device Lock Service using **Typical setup** or you can install only Device Lock Manager using **Custom setup** then selecting the *Device Lock Manager* component.

After a successful install, you can run Device Lock Manager by selecting the **Device Lock Manager** item from the **Programs…** menu.

Copyright ©1997-2004 SmartLine Inc. All rights reserved.

2.2 — Interface

Device Lock Manager has a user-friendly, easy-to-use interface. All functions can be accessed with either a mouse or keyboard.

In any dialog, you can press the F1 button to get specific help.

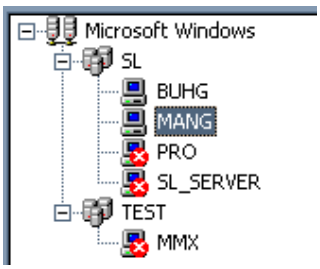
The main window of Device Lock Manager can be resized. Device Lock Manager saves its size and position and restores these at its next startup.

Device Lock Manager has a menu at the top of its main window through which most functions are accessible.

You can select **Always on Top** from the **View** menu to keep the Device Lock Manager on top any other applications (always displayed on the screen).

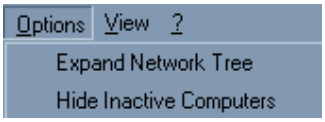
2.3 — Main Dialog

When you start Device Lock Manager, it displays the main dialog where you can select a computer to control.



The left side of the main dialog shows a list of the computers available in your network. This list is called the computer tree. Each computer running Device Lock Service has an icon. Each computer without Device Lock Service running has an icon of a computer overlaid by a red circle containing a white **X**, indicating the computer is inactive for Device Lock. If **Check Computers** in the **Options...** menu is not selected, Device Lock Manager does not check Device Lock Service on each computer and all computers have the same icon.

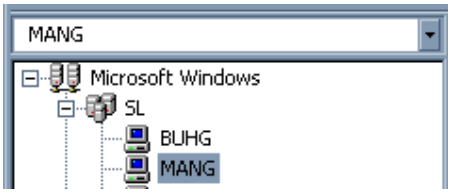
If you want a listing of only active computers — computers with running and accessible Device Lock Service — select **Check Computers** and **Hide Inactive Computers** in the **Options...** menu. If you want the computer tree to expand automatically, select **Expand Network Tree** in the **Options...** menu.



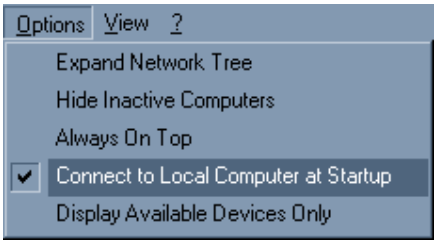
To refresh a list of computers, press F5 or select **Refresh Network Tree** from the **View...** menu. Also, you can refresh the state (whether active or inactive) of a selected computer by pressing Shift+F5 or selecting **Refresh Selected Computer** from the **View...** menu.

If your computer is not connected to a network, the list of computers will be empty or may contain only a single record — "Microsoft Windows Network" (or similar message).

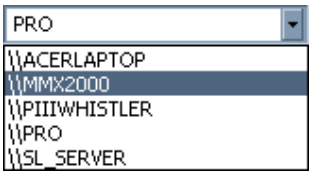
To access a remote computer, it needs to have Device Lock Service installed and running, and it needs to have a connection to your computer. To access a remote computer, select it from the computer tree. Device Lock Manager automatically connects to the computer after it has been selected. To select a system, use the mouse to select the computer or use the keyboard's arrow keys and press ENTER. Alternatively, you can type in the computer name in the field above the computer tree and press ENTER.



To connect to the local computer, do not specify a computer name. If **Connect to Local Computer at Startup** is enabled in the **Options...** menu, Device Lock Manager automatically connects to the local computer each time it starts up.

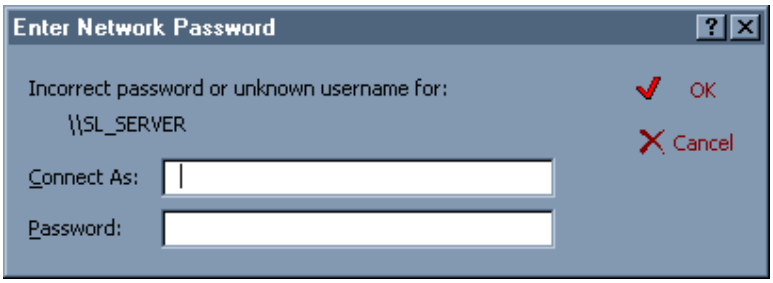


Copyright ©1997-2004 SmartLine Inc. All rights reserved.

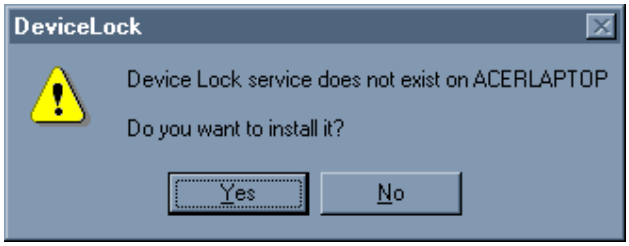


All frequently used computers are added automatically to the most recently used (MRU) list so they can be easily accessed.

If you don't have administrative privileges on a selected computer, Device Lock Manager displays the Enter Network Password dialog and you'll be able to connect under the account of any other user. The Enter Network Password dialog appears when you attempt to connect to a computer, but the domain controller (DC) does not recognize the user account you have used to log on. This often occurs when you are logged on as the administrator of a local computer and attempt to access domain resources. To access the domain resources, you must provide a valid user account and password that the domain recognizes. User accounts are domain name followed by a backslash (\) and the user name, e.g. *D1\John*.

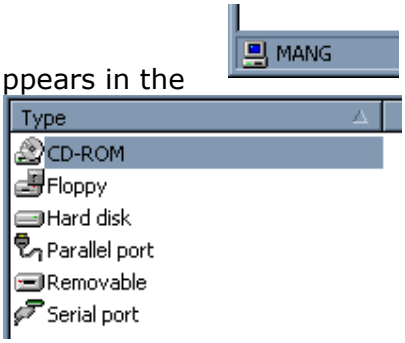


Device Lock Service should be installed on the computer so you can control the access to devices on that computer. Device Lock supports remote installing. This lets a Systems Administrator set up a service on distant machines without having to physically go to them. If the Device Lock Service isn't installed on the remote system to which you are connecting, Device Lock Manager suggests that you install the service. Select the Device Lock Service executable file (*dlservice.exe*) and Device Lock Manager copies it to the remote computer's Windows system directory (e.g. *c:\winnt\system32*). If the service is on the client system, but is outdated, Device Lock Manager replaces it.



Device Lock Manager automatically starts Device Lock Service if it's stopped on the system.

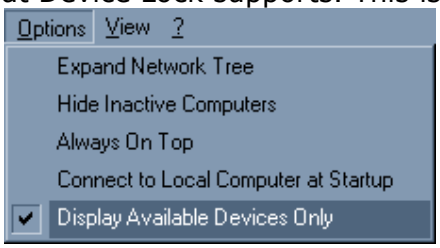
If you successfully connect to a computer, its name appears in the status bar of Device Lock Manager. Device Lock Manager functions become available only if you are connected to a computer.



The list of device types (**Floppy**, **Removable**, **Serial port**, etc.) appears at the top-right side of the main dialog.

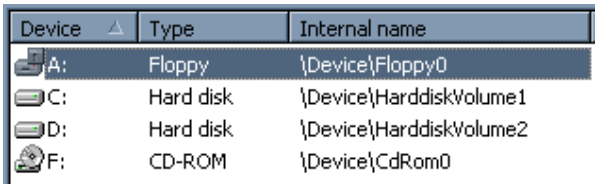
Copyright ©1997-2004 SmartLine Inc. All rights reserved.

If **Display Available Devices Only** is enabled in the **Options...** menu, Device Lock Manager shows only those devices currently available from your computer. Otherwise, you will see every type of device that Device Lock supports. This is useful when you want to set permissions to devices that are not yet installed or are currently unplugged from the computer.



NOTE: Device Lock Service automatically detects new devices and sets permissions (if any) for them. Device Lock Service recognizes new devices, not by their user-mode names or letters (such as A:, COM1) but by their internal names (such as \Device\Floppy0, \Device\Serial0) so it works even with unnamed devices.

To set permissions for a device type, highlight it (use CTRL and/or SHIFT to select several types simultaneously) and select **Set Permissions** from the **File...** menu or press F2. Alternatively, you can press the appropriate button at the top-right side of the main dialog box. Below the list of types, Device Lock Manager displays the devices that are available for a selected device type. In this list, you can see the devices that are currently available for local users on the remote computer. If there are no devices currently available for the selected type, this list is empty. To see a listing of all the devices that are available to the remote computer, select all records in the list of types.

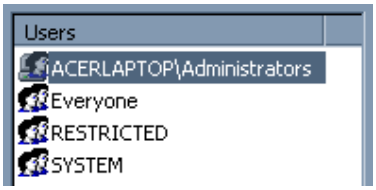


Device	Type	Internal name
A:	Floppy	\Device\Floppy0
C:	Hard disk	\Device\HarddiskVolume1
D:	Hard disk	\Device\HarddiskVolume2
F:	CD-ROM	\Device\CdRom0

NOTE: When you set permissions for a device type, you set these permissions for every device belonging to that type. It is impossible to set different permissions for two different devices if they are of the same type (e.g. both are floppy drives).

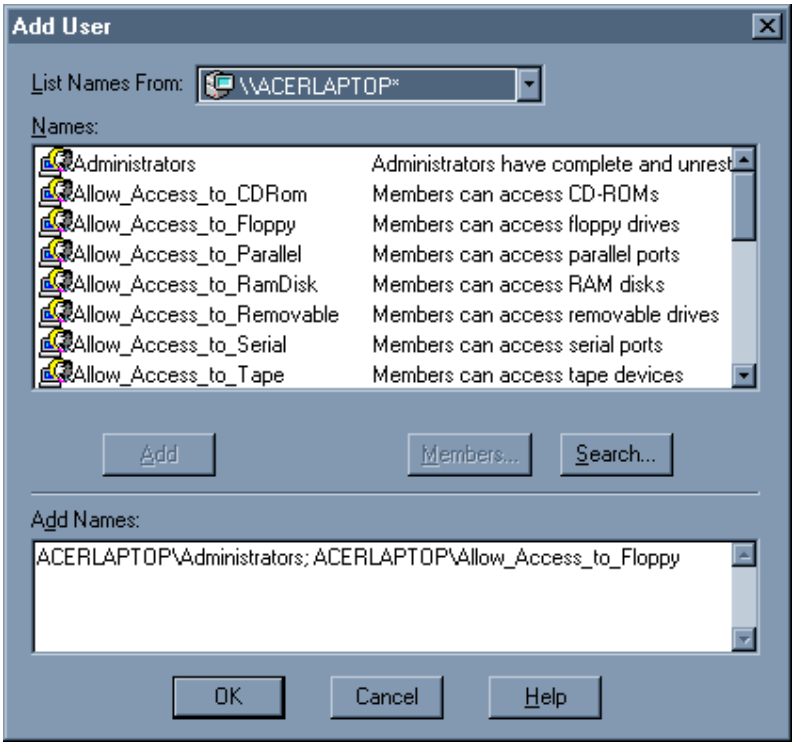
2.4 — Permissions Dialog

This dialog controls access to devices. Set permissions to a device type or to a group of types and define the users and times (day of the month and/or day of the week) each can be accessed.



The names of the users and user groups assigned to a device type are shown in the list of accounts at the left-hand side of the permissions dialog.

To add a new user or user group to the list of accounts, click on the **Add** button. You can add several accounts simultaneously.



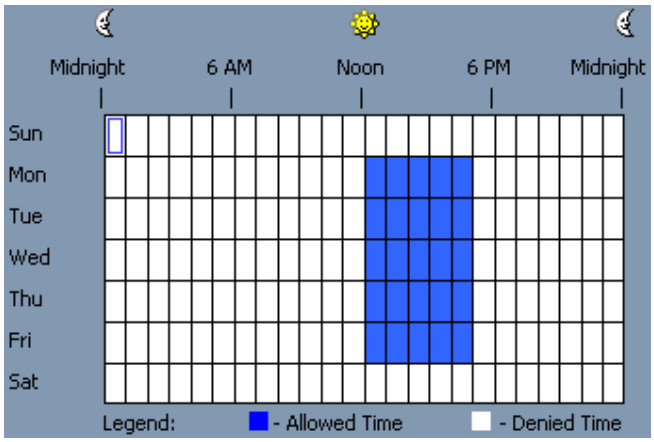
To delete a record from the list of accounts, use the **Delete** button.

Use the **Set Default** button to set default permissions for devices. Default permissions are enabled by using the following access selections:

- The Everyone account has Full Access rights except for the Allow Format privilege.
- Members of the Administrators group and the SYSTEM account have Full Access rights, including the Allow Format and Allow Eject privileges.

Copyright ©1997-2004 SmartLine Inc. All rights reserved.

Using special time control, you can define a time when a selected user or user group will or will not have access to devices. **Time control** appears at the top-right side of the permissions dialog. Use the left mouse button and select the allowed time. To select a denied time, use the right mouse button. Also, you can use the keyboard to set times — arrow keys for navigation and the spacebar to toggle allowed/denied time.
NOTE: each user can have his/her own allowed/denied time.



To define which actions on devices are to be allowed for a user or user group, set the appropriate rights and privileges:

- **Full access** – to enable the reading, writing, deleting, executing, etc. of files and directories.
- **Read-only** – to enable only the reading of files and directories.
  NOTE: "Read-only" means "No access" for tape devices, WiFi, Bluetooth, USB, FireWire, infrared, and serial and parallel ports.
- **Allow Format** – to enable the formatting, checking, and any other direct access of drives.
  NOTE: You can enable this privilege only if Full Access is selected. This privilege is not available for CD-ROMs, DVDs, tape devices, WiFi, Bluetooth, USB, FireWire, infrared, or serial and parallel ports.
- **Allow Eject** – to enable ejection of the media.
  NOTE: You can enable this privilege only if Full Access is selected. This privilege controls only ejection via software. Hardware ejection using the Eject button on a device's front panel cannot be prevented.
- **No access** – user cannot access a device.

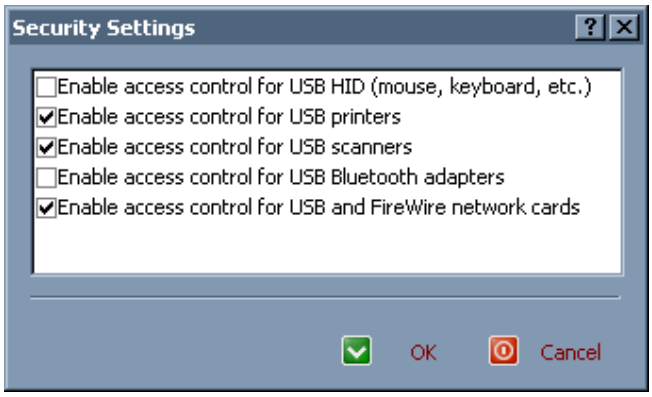
NOTE: When you set permissions to WiFi and Bluetooth adapters, it not affects existing connections.

If you want to deny all actions for a selected user or user group, you must select **No Access**. Also, to deny all actions, you can set the denied time for all periods.

To deny access to devices for all users and user groups, add only the Everyone user to an account's list and select **No access** or set the denied time for all periods. Also, you can remove all records from an account's list and set empty permissions so nobody can access devices.

Copyright ©1997-2004 SmartLine Inc. All rights reserved.

For USB and FireWire ports, you can define additional security parameters. Press the **Security Settings** button to define security parameters, such as:


Security Settings
Enable access control for USB HID (mouse, keyboard, etc.)
Enable access control for USB printers
Enable access control for USB scanners
Enable access control for USB Bluetooth adapters
Enable access control for USB and FireWire network cards
OK
Cancel

- **Enable access control for USB HID** - if checked, allows Device Lock Service to control access to Human Input Devices (mouse, keyboard, etc.) plugged into the USB port. Otherwise, even if the USB port is locked, Human Input Devices continue to function as usual.

- **Enable access control for USB printers** - if checked, allows Device Lock Service to control access to printers plugged into the USB port. Otherwise, even if the USB port is locked, printers continue to function as usual.

- **Enable access control for USB scanners** - if checked, allows Device Lock Service to control access to scanners plugged into the USB port. Otherwise, even if the USB port is locked, scanners continue to function as usual. ***NOTE: Some USB digital cameras with the DPOF (Digital Print Order Format) support are recognized by Windows as scanners.***

- **Enable access control for USB Bluetooth adapters** - if checked, allows Device Lock Service to control access to Bluetooth adapters plugged into the USB port. Otherwise, even if the USB port is locked, Bluetooth adapters continue to function as usual.

- **Enable access control for USB and FireWire network cards** - if checked, allows Device Lock Service to control access to network cards plugged into the USB or FireWire (IEEE 1394) port. Otherwise, even if the USB or FireWire port is locked, network cards continue to function as usual.

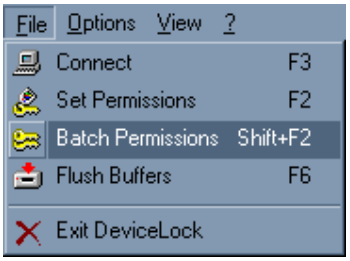
These security parameters enable you to completely lock USB and FireWire ports, but allow the usage of some devices. For example, you can disallow using all the USB devices except the mouse and keyboard.

Copyright ©1997-2004 SmartLine Inc. All rights reserved.

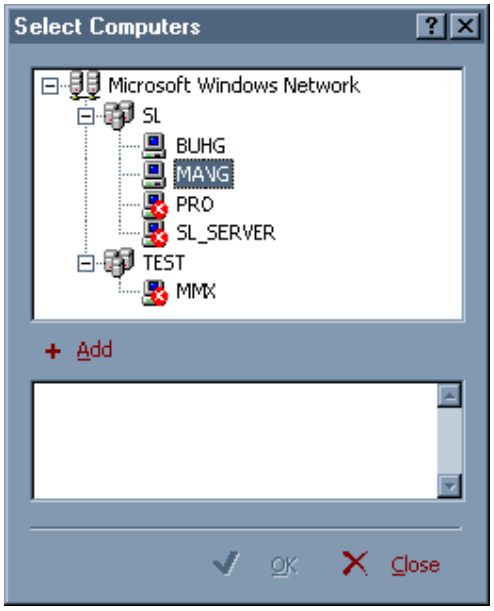
2.5 — Batch Permissions

Batch Permissions is a powerful and useful function. Midsize and large networks contain many similar computers with similar devices (e.g. all computers have floppy drives and CD-ROMs) and Batch Permissions allow network administrators to set permissions for all of them quickly and uniformly.

Batch Permissions is available once Device Lock Manager is loaded. You do not need to connect to any computer directly to use this function.
NOTE: Any permission you set using Batch Permissions overwrites all previously assigned permissions on those devices individually.



To access Batch Permissions, select **Batch Permissions** from the **File...** menu, press Shift+F2, or press the appropriate button at the top, right-side of the main dialog.



You must select the computers that you want to include in the batch processing. To add computers to the list, press the **Add** button. This opens a dialog with the computer tree where you can select any computer available on your network. Double-click the computer name in the computer tree to add this computer or type the computer's name manually and press the **OK** button to include selected computers to the list.

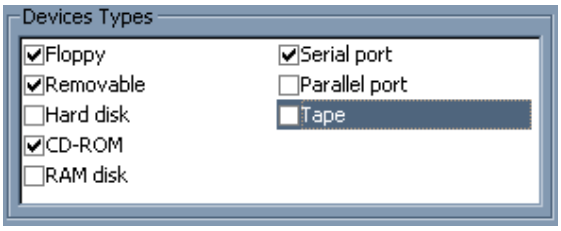
Also, you can load computers from an external file. Press the **Load** button and select a file that contains the list of computers. Two file formats are supported — text file (.txt) and comma separated values (.csv). A text file must contain each computer's name on separate lines. Computer names in a .csv file must be separated by commas or semicolons.

To save a computer listing to an external file, press the **Save** button, then select the type of the file — .txt or .csv.

If you want Device Lock Service to be automatically installing on the computers selected for the batch processing, check **Install/Update Service** at the left-bottom side of the dialog. If the service is on the computer, but is outdated, Device Lock Manager updates it.

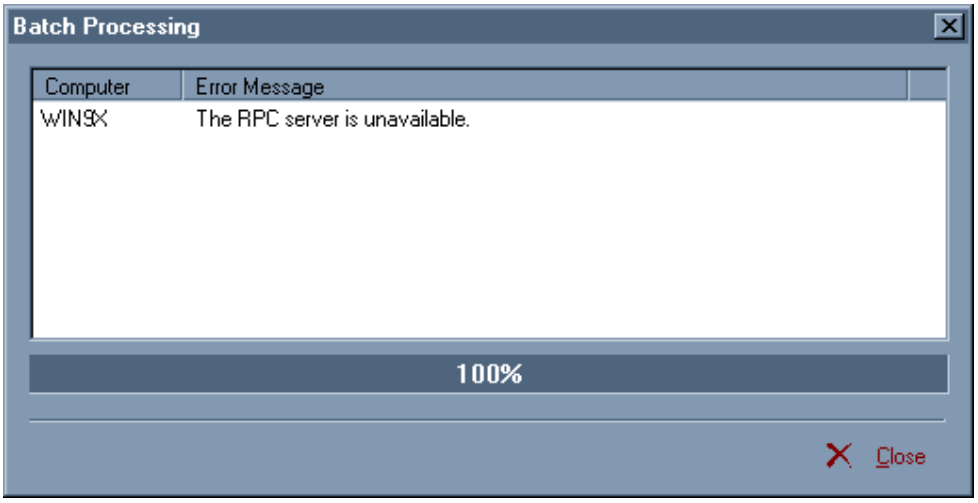
Add users or user groups to the account's list. Define allowed/denied times on the time control and set the appropriate rights and privileges for each user and user group as described in **Section 2.4**.

Copyright ©1997-2004 SmartLine Inc. All rights reserved.



The final step is selecting the devices you want to process. There are few types of devices available in the Device Lock Manager: Floppy, Removable, CD-ROM, and so on. Each of these types represents all the devices of this category, i.e. Floppy represents all floppy drives that are available on the computer; Removable — all removable drives, and so on.

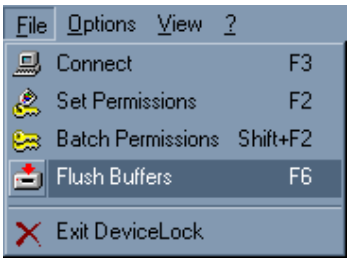
To start batch processing, press the **Set Permissions** button.



2.6 — Flush Buffers

Device Lock can save a disk's cache and unsaved buffers to selected device.

To flush the buffers, highlight the device in the devices list (use CTRL or/and SHIFT to select several devices simultaneously) and then select **Flush Buffers** from the **File...** menu, press F6 or press the appropriate button at the bottom-right side of the main dialog. **Flush Buffers** is available only for devices that support write-operations, e.g. floppies, ZIPs, JAZZs, etc. **Flush Buffers** cannot be used for devices such as CD-ROMs.



NOTE: If you select a device with a removable media, make sure that this device has the media inserted and isn't marked as read-only.

Flush Buffers is very useful for removable medias, i.e. floppies, ZIPs, Magneto-Optical disks, etc. It can prevent your data from being lost because of a write-behind cache. Windows gives you the option to use write-behind caching to improve the performance of removable disk drives, but sometimes it may be a reason for data loss on those drives. It is recommended to force the flushing of a disk's cache from time to time, especially before ejecting disks.

Copyright ©1997-2004 SmartLine Inc. All rights reserved.

3.1 — Installation

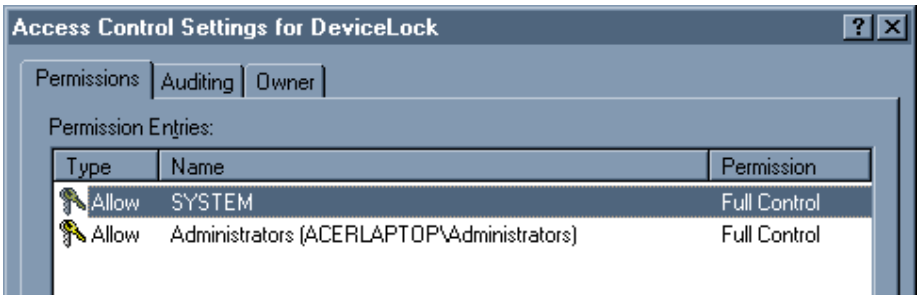
Device Lock Service can be installed on any computer running Windows NT/2000/XP or Windows Server 2003.

To install Device Lock Service run Setup (*setup.exe*).

Device Lock Service installs to the directory of your choice. Setup tries to find a Device Lock Service installation and if one exists, Setup suggests that you install Device Lock Service to the same directory. If a previous installation does not exist, Setup suggests that Device Lock Service be installed to the Program Files directory on the system drive (e.g. *C:\Program Files\Device Lock*). In any case, you can select another directory for installation.

You have the following two choices: either install both Device Lock Service and Device Lock Manager using **Typical** setup or install only Device Lock Service using **Custom** setup and select the **Device Lock Service** component.

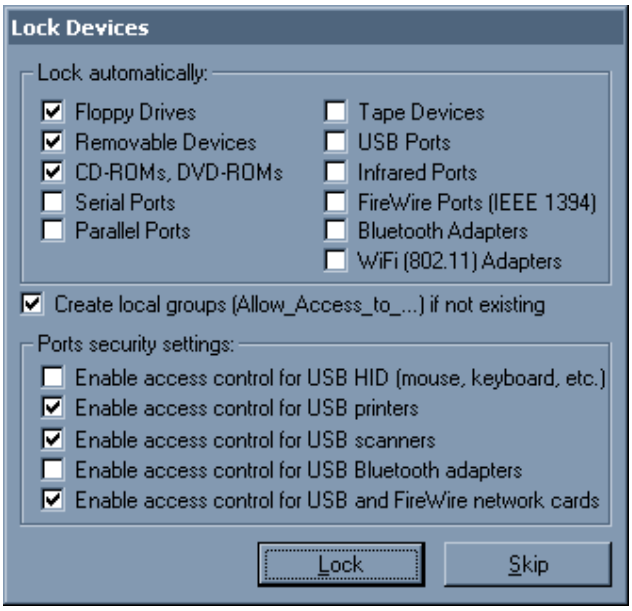
If you install Device Lock on an NTFS partition, Setup protects Device Lock's directory and files by allowing only members of the Administrators group or the SYSTEM account to access Device Lock's files or to uninstall Device Lock.



Setup protects Device Lock Service by allowing only members of the Administrators group or the SYSTEM account to start, stop, or delete the service.

Copyright ©1997-2004 SmartLine Inc. All rights reserved.

During the installation, Setup suggests that you set permissions to the local devices. Check the **Create local groups if not existing** checkbox and Setup will create the special local user group Allow_Access_To_ for each device type (e.g. Allow_Access_To_Floppy for floppy drives), if these do not exist on the local computer. Select the devices you would like to automatically lock during installation and press the **Lock** button. Setup assigns the Full Access right including the Allow Format and Allow Eject privileges for members of the Administrators group and the SYSTEM account. Members of the Allow_Access_To_ group will have the Full Access right, including the Allow Eject privilege, but without Allow Format.



Check **Enable access control for USB HID**, **Enable access control for USB printers Enable access control for USB scanners** or **Enable access control for USB Bluetooth adapters** to allow Device Lock Service to control security for Human Input Devices (mouse, keyboard, etc.), printers, scanners or Bluetooth adapters plugged into the USB port. To allow access control for USB and FireWire network cards, check **Enable access control for USB and FireWire network cards**. Otherwise, even if ports (USB and/or FireWire) are locked, these devices continue to function as usual.
NOTE: Some USB digital cameras with the DPOF (Digital Print Order Format) support are recognized by Windows as scanners.

Press the **Skip** button if you prefer to wait until after installation to set permissions to these devices using Device Lock Manager.

Setup also supports unattended (silent) setups. This provides an installation method that can be used from within a batch file. To install Device Lock Service without user intervention, run Setup with the */s* parameter (e.g. *c:\setup.exe /s*). There is a special configuration file for silent setups named *Device Lock.ini*. *Device Lock.ini* must be in the same directory where *setup.exe* is located. With this file, you can customize the installation parameters. For example, to install only Device Lock Service, *Device Lock.ini* should look like:

[Install]
Service = 1
Manager = 0
Documents = 0

To automatically lock devices during installation, specify the Lock Devices parameters. Only members of the special local user group Allow_Access_to_, the operating system (SYSTEM) and the local administrators have access to devices:

Copyright ©1997-2004 SmartLine Inc. All rights reserved.

[Lock Devices]
Floppy = 1
Removable = 1
CDROM = 1
Serial = 1
Parallel = 1
Tape = 1
USB = 1
IRDA = 1
FireWire = 1
Bluetooth = 1
WiFi = 1

Setup assigns the Full Access right, including the Allow Format and Allow Eject privileges for the operating system (*SYSTEM*) and the local administrators.

If the *CreateGroups* parameter is enabled, Setup creates the special local user group Allow_Access_To_ for each device type (e.g. Allow_Access_To_Floppy for floppy drives), if these do not exist on the local computer. Members of the Allow_Access_To_ group have the Full Access right, including the Allow Eject privilege, but without Allow Format. If the *CreateGroups* parameter is disabled and the special group does not exist on the local computer, only the operating system and the local administrators have access to the device.

In the *AccessTo...* parameter, you can specify an additional account (user name, local or global group) to have access to a device (e.g. *AccessToFloppy* for floppy drives):

AccessToFloppy = D1\John

Setup assigns the Full Access right, including the Allow Format and Allow Eject privileges for the account specified in this parameter.
NOTE: The account must exist before it can be assigned to a device type.

If *CtrlUSBHID*, *CtrlUSBPrint*, *CtrlUSBScan* and *CtrlUSBBth* parameters are enabled, Device Lock controls access to Human Input Devices (mouse, keyboard), printers, scanners, and Bluetooth adapters plugged into the USB port. If the *CtrlFWNet* parameter is enabled, Device Lock controls access to network cards plugged into the USB and/or FireWire (IEEE 1394) port. Otherwise, even if ports are locked, these devices continue to function as usual. This enables you to completely lock USB and FireWire ports but allow the usage of some devices (e.g. USB mouse).

If you have purchased a license for Device Lock, you can also specify the location of its license key file in the *Device Lock.ini* file so Setup automatically registers new versions of a service:

RegFileDir = C:\Directory

where *C:\Directory* is where your license key file is located.

You can also specify a destination directory for Device Lock:

InstallDir = C:\Program Files\Device Lock

If you want to run a program (e.g. batch file) after a successful install, you can specify the *Run* parameter:

[Misc]
Run = C:\mybatchfile.bat

Device Lock supports remote installation to help system administrators set up a service on remote machines without ever having to physically go to them. If the Device Lock Service isn't installed on a remote, Device Lock Manager will suggest that you install the service. Select the Device Lock Service executable file (*dlservice.exe*) and Device Lock Manager will copy it to the remote computer. The Device Lock Service executable file will be copied to the Windows system directory (e.g. *c:\winnt\system32*) if this service doesn't exist on this system. If the service exists on this system but is too old, Device Lock Manager will copy the executable file to the directory of the old file and the old file will be replaced.

Device Lock can also be installed using Microsoft Systems Management Server (SMS). Use the package definition files (*DevLock.pdf* for SMS version 1.x and *DevLock.sms* for SMS version 2.0 and later) supplied with Device Lock, located in the *sms.zip* file.

Copyright ©1997-2004 SmartLine Inc. All rights reserved.

Appendix

Permission Examples

a) To prevent anyone from accessing a device at any time:

   Add the Everyone user to an account list and select the **No Access** right or select the **Full Access** right and set the denied time to all periods. Alternatively, you can remove all records from an account list and set empty permissions.

b) To prevent anyone from accessing the USB port, but allow the USB mouse and keyboard:

   Add the Everyone user to an account list and select the **No Access** right or select the **Full Access** right and set the denied time to all periods. Open the **Security Settings** dialog (press the **Security Settings** button on the **Permissions** dialog) and clear the **Enable access control for USB HID** parameter.

c) For anyone to read floppy disks, but only members of the *Administrators* group to write data to the media:

   Add only the Everyone user and the Administrators local group to an account list, select **Full Access** for Administrators and **Read-only** for Everyone, then set the allowed time for all periods for each record in the account list.

d) For only members of the Administrators group and the SYSTEM account to access a device at any time:

   Add only the SYSTEM user and the Administrators local group to an account list, select the **Full Access** right and set the allowed time for all periods for each record in the account list.

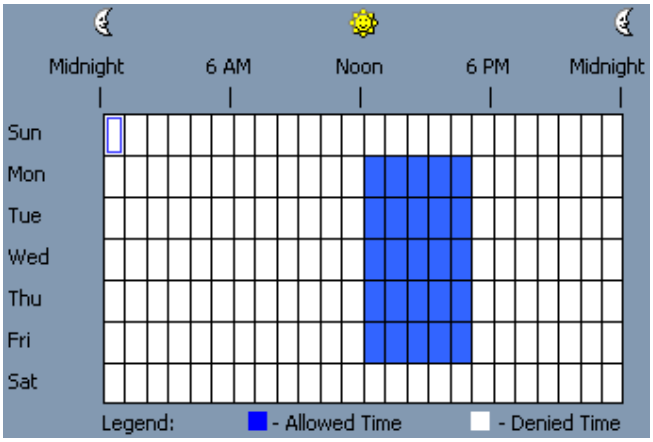
e) For anyone can access a device at any time, but only members of the Administrators group to perform formatting and checking of the media of the device:

   Add only the Everyone user and the Administrators local group to an account list, select the **Full Access** right, and set the allowed time for all periods for each record in the account list. Uncheck the **Allow Format** privilege for the Everyone user and check this privilege for the Administrators group.

Copyright ©1997-2004 SmartLine Inc. All rights reserved. — Ecora Software — Device Lock User Manual —

f) For members of the Users group to access a device only from Monday till Friday and between 12pm and 5pm, but Administrator to access this device at any time:

Add only the Users local group and the Administrator user to an account list and select the **Full Access** right for each. Set the allowed time for all periods for the Administrator user. Set the time as shown on the picture below for the Users group.



NOTE: The Administrator user must not belong to the Users group.